ENTENDIENDO EL SGSI

Andrade Rodríguez, Yovany Andrés
andres.andrader@outlook.com
Universidad Piloto de Colombia

Abstract— This article is made as deliverable Applied Research Seminar from the Pilot University of Colombia, for the program Computer Security Specialization C26, is a brief compilation of basic concepts to consider for application creation SGSI at any scale, and the minimum issues to consider when entering a to the formulation of an SGSI are addressed, a brief summary of the framework COBIT, ISO 27000 standard gives rules and ITIL V3 currently available in the industry, which allow an implementation of the SGSI within the best practices recommended and most used, in addition to that is done a comparison between the three methods to extract the pros and cons of each, addressing a globally common errors that might present during such deployments.

Resumen— Este artículo es realizado como entregable del Seminario de investigación aplicada de la Universidad Piloto de Colombia, para el programa de Especialización de Seguridad Informática C26, es una breve recopilación de conceptos básicos que se deben tener en cuenta para ser aplicados en la creación de un SGSI a cualquier escala, y se abordan los temas mínimo que se deben tener en cuenta .a la hora de entrar a la formulación de un SGSI, se da un breve resumen acerca del marco de referencia COBIT, normas ISO 27000 y estándar ITIL V3 disponibles actualmente en la industria, los cuales permiten realizar una implementación del SGSI dentro de las mejores prácticas, recomendadas, y más utilizadas, además a eso se realiza un comparativo entre las 3 metodologías para extraer los pros y contras de cada una, abordando de una manera global los errores comunes que se pueden llegar a presentar durante este tipo de implementaciones.

Índice de Términos — SGSI, COBIT, ISO 27000, ITIL V3, PDCA, holística.

I. INTRODUCCIÓN

Durante el proceso de formación recibido por parte de la Universidad Piloto de Colombia en el programa de Seguridad Informática y específicamente en el Seminario de Investigación aplicada, finalizando el proceso de formación he escogido dar un resumen y opinión personal, acerca de 3 metodologías vistas durante el proceso de formación, las cuales me llamaron la atención debido a que son el pilar de los procesos para la implementación de un SGSI (Sistemas de Gestión de Seguridad de la Información), en una empresa sin importar si es grande o pequeña, a través del articulo deseo retomar los conceptos vistos durante los módulos del SIA, así como los vistos durante las especialización, dar un concepto personal, mediante el cual dar una guía de consulta práctica, rápida y sencilla, donde se evidencian los pasos básicos que se deben tener en cuenta para establecer un proceso para la seguridad de la información y no morir en el intento, teniendo como base conceptos puntuales, muy sencillos, aplicables en la práctica, que nos ayuden en la construcción de cualquier política, proceso y/o directriz, en el entorno real de una empresa.

II. ¿PARA QUÉ NECESITAMOS UN SGSI?

Todos los días tenemos riegos que atentan contra la seguridad de la información, en nuestra vida diaria, teniendo en cuenta que día tras día el avance en la tecnología y el abaratamiento de los costos nos permiten estar conectados todo el tiempo a internet, redes sociales, transacciones en línea, trabajo remoto y cooperativo a través de internet, los cuales no son ajenos en el entorno corporativo, por ende estos riesgos los trasladamos directamente a nuestro

entorno de trabajo, afectando a nivel gerencial, financiero y operativo la empresa donde desempeñemos nuestro trabajo, esto se traducen en potenciales perdidas de recursos, tiempo y dinero, estos riesgos los vemos día a día representados por [1]:

Usuario internos | Usuarios externos | Eventos fuera de control y/o fortuitos.

Teniendo en cuenta esto factores las empresas necesitan:

- Conocer
- Gestionar
- Minimizar

Para:

- Alinear TI con el negocio.
- Lograr una buena relación costo/beneficio asegurando el máximo rendimiento con la inversión en TI.
- Mantener la seguridad de la información.
- Mantener la operación de TI.
- Cumplir con requerimientos regulatorios y contractuales.
- Analizar y ordenar la estructura de los sistemas de información.
- Establecer los procedimientos de trabajo para mantener la seguridad.
- Disponer de controles para medir.

Todos aquellos riesgos que atentan contra la seguridad de la información [1], para alcanzar un nivel de riesgo menor que el soportado por la empresa, para preservar la confidencialidad, integridad y disponibilidad de la información.

III. ¿QUÉ DEBE TENER UNA EMPRESA?

Lo primero que necesitamos tener en cuenta es formular las siguientes preguntas:

- ¿Dónde está la empresa?
- ¿Qué recursos tiene?
- ¿Adónde quiere llegar?
- ¿Qué es lo que realmente necesita?

Para iniciar la construcción de una estrategia que le permita implementar los procesos.

Fig. 1 Construcción de la estrategia.
Imagen tomada del sitio: http://www.magazcitum.com.mx/wp-content/gallery/magazcitum-212-4/hectoracevedo_iso_fig_3.jpg

Existen a nivel mundial Normas, Estándares y marcos de referencia, que son base para la generación de directrices que permitan construir procesos eficientes, eficaces y lo más importante aplicables, tales como:

ISO/IEC-27001 (Information technology – Security techniques – Information security management systems – Requirements) Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). [2]

COBIT (Control Objectives Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan.

ITIL v3. Es un conjunto de buenas prácticas destinadas a mejorar la gestión y provisión de servicios TI.

- ISO 27001 y 27002 como Norma o Estándar se sitúan en el mayor nivel de cumplimiento
- COBIT se basa en prácticas para garantizar el gobierno de TI lo colocamos en un nivel medio de cumplimiento ya que basado en normas y estándares es como se implementa el correcto gobierno de TI.
- ITIL dentro del bajo nivel de cumplimiento ya que este marco de servicio solo pretende habilitar el servicio y no garantizar su operación.

Mientras mayor es el cumplimiento vemos que necesitamos el uso de Normas como ISO 27001 e ISO 27002, para asegurar ese nivel de cumplimiento necesitamos implementar un marco de control como COBIT ya que convive de manera natural con las normas de la familia ISO 27000, un correcto marco de servicios, como ITIL.

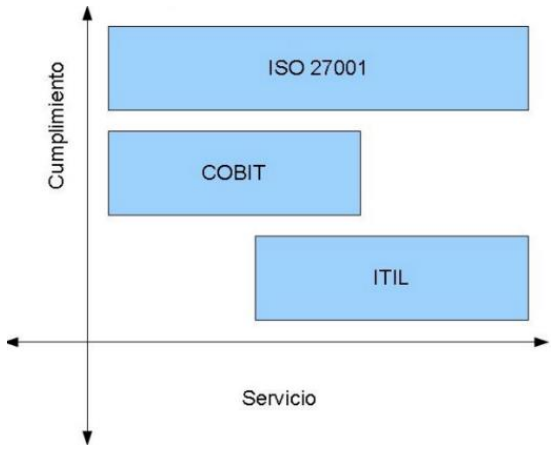

Fig. 2 Cumplimiento vs. Servicio
Imagen tomada del sitio: http://3.bp.blogspot.com/-5X1qq8ic7p8/TjsPEL0ue7I/AAAAAAAAAD0/_OphlGy6nOU/s1600/figura1.jpg

- Necesitamos el uso de Normas como ISO 27001 e ISO 27002, para asegurar un nivel de cumplimiento estandarizado.
- Necesitamos implementar un marco de control como COBIT ya que convive de manera natural con las normas de la familia ISO 27000.
- Un correcto marco de servicios, como ITIL, solo se utiliza para garantizar la satisfacción del cliente y el buen uso de los recursos de tecnología.

IV. ¿QUÉ MARCO DE REFERENCIA, NORMA O ESTÁNDAR DEBERÍA UTILIZAR?

En primera instancia el uso de la Norma ISO 27001 e ISO 27002 para asegurar el cumplimiento
En segunda instancia COBIT servirá para: evaluar, formular, definir y justificar, auditar [3].
En tercera instancia, ITIL, cuando se necesitan más detalles, o cuando necesito la autoridad para justificar lo que sugiero.

Las razones para que esto sea así son:
- COBIT es más completo y sistemático, sirve para planear, organizar, dirigir y controlar toda la función informática dentro de una empresa. Actúa sobre la dirigencia y ayuda a estandarizar la organización.
- "COBIT define qué debemos controlar e ITIL define cómo debemos hacerlo".
- ITIL actúa sobre los procesos y, a través del conjunto de buenas prácticas que lo conforman, mejorar el servicio que ofrece la empresa y medirlos (para una mejora continua).

V. FORTALEZAS Y DEBILIDADES DE CADA UNO

- ISO 27000, es bastante fuerte en los controles de seguridad, pero NO detalla el "Como hacer".
- COBIT está principalmente contemplado para los controles y las métricas, El "Como hacer".
- NO es fuerte en temas de seguridad.
- ITIL su diseño es fuerte en procesos, tiene limitaciones en la construcción de sistemas de seguridad, es decir se enfoca mucho en el "Hacer".

VI. VENTAJAS DE TRABAJAR COMBINANDO ISO27000, COBIT E ITIL

Una integración de ambos marcos derivará en el cumplimiento eficiente de las regulaciones que se les exige a las organizaciones [4].

- COBIT E Itil comparten muchos procesos comunes.
- COBIT e Itil v3 están diseñados en el ciclo de vida de las aplicaciones, sistemas y servicios de TI.
- COBIT, ITIL e ISO-27000 tiene presupuestado ciclos de mejora continua (PDCA).
- Las últimas versiones de cada uno tomaron en cuenta a los otros para estar "alienados lo mejor posible".
- Los controles de Cobit e ISO-27000 son enfocados a la seguridad de la información.

VII. RECOMENDACIÓN PARA LA IMPLEMENTACIÓN DEL "SGSI"

Después de haber definido el estándar, norma y/o narco de referencia que se va a utilizar, la empresa debe tener en cuenta que debe seguir los siguientes pasos para la implementación de la directriz [5], como mínimo.

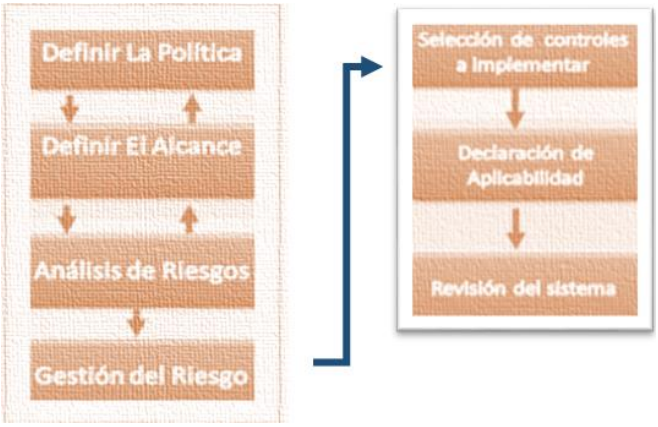

Fig.3 Componentes SGSI
Imagen tomada del sitio: http://normas-iso.com/wp-content/uploads/2012/02/SGSI.png

Descripción de cada uno de los pasos

Definir la Política: Recopilar las directrices que debe seguir la seguridad de la información de acuerdo a las necesidades de la empresa teniendo en cuenta la legislación vigente.

Alcance: Se determinar los procesos más críticos de la empresa, definir que se quiere proteger y un punto de partida. Se deben definir las actividades de la empresa, ubicación física, la tecnología con la que se cuenta en la organización y las áreas, procesos y locaciones que se van a excluir.

Análisis de Riesgos: Gestión del riesgo desde el punto de vista organizacional, se debe tener en cuenta el análisis de activos de información (las amenazas y vulnerabilidades se generara el análisis de riesgos.

Gestión del Riesgo: Grado de aseguramiento requerido y soportado por la empresa, se generara resultados y conclusiones.

Selección de controles a Implementar: Controles propuestos por norma, también tener en cuenta controles adicionales que puedan surgir por obligación y/o necesidad, en este punto surgen una lista de controles seleccionados.

Declaración de Aplicabilidad: Controles propuestos por la norma, nuevamente en este punto surgen una lista de controles selecciones.

Revisión del Sistema: Medida preventivas y correctivas, de las cuales surgen propuestas de mejora.

Estas fases deben ir siempre soportadas por la auditoria interna, y con un plan de auditorías asociado a la implementación del estándar, marco de referencia o norma seleccionada.

Como recomendación el sistema debe siempre verse de manera holística, para poder hacer una verdadera integración global y total en la empresa, de las cuales evidenciamos el siguiente aspecto:

Interconexiones dinámicas

Estas están encargadas de enlazar todos los elementos los cuales ejercen fuerza multidireccional que empuja y atrae a medida que combinan las situaciones [6].

Gobierno: Dirección de la empresa la cual exige liderazgo estratégico, el cual establece el límite dentro de los que opera la empresa, se debe implementar dentro de los procesos para monitorear el rendimiento, es la que se encarga de velar:

- Por el cumplimiento de los controles y regulaciones.
- Asegurar que se determinen y definan los objetivos.
- Gestionar los riesgos apropiadamente.
- Se encarga de que los recursos de la empresa sean bien utilizados.

Cultural: Patrón de conductas, convicciones, supuestos, actitudes, maneras de hacer las cosas propias de la empresa.

Comportamiento → Reglas NO escritas → Estándares compartidos por los empleados.

Niveles del comportamiento que debemos tener en cuenta [7]:

Nacional: Legislación, regulación, política y tradiciones.

Organizacional: Políticas internas, estilo jerárquico y expectativa.

Social: Familiar, cultural y etiquetas de la región de donde es oriundo el individuo.

Habilitación y Soporte: Interconexión dinámica tecnológica y de los procesos, para garantizar que los procesos sean prácticos y fáciles de usar.

Seguimiento: Afloramiento, desarrollo, crecimiento y evolución.

Este patrón surge durante el proceso de implementación en la vida de la empresa, estos resultados NO son predecibles.

Factores Humanos: Tecnología ←→ Gente.

Puede llegar a existir una mala interacción entre la gente y la tecnología, puede llegar a causar problemas mayores como: fuga de información, robo, mal uso.

Se requiere tener en cuenta y programar capacitación na diferentes niveles.

VIII. ASPECTOS DE SEGURIDAD RECOMENDADOS EN EL SGSI

La estrategia debe arrancar por una o varias políticas de seguridad, las cuales tienen como fin principal la organización de la información, mediante la gestión de activos y el control de acceso, se debe tener en cuenta la seguridad física y del entorno, así como la seguridad en los recursos humanos para su contratación y capacitación, que de una o de otra forma siempre va a hacer el eslabón más débil de la cadena, y de ahí partimos para decir que no existe la seguridad completa [9].

El SGSI con una política o varias políticas estructuradas realizara una gestión autónoma y en proceso de mejora continua en los siguientes ítems.

- Gestión de los incidentes de seguridad de la información.
- Gestión de la continuidad del negocio.
- Gestión de las comunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.

IX. RETOS Y DESAFÍOS QUE SE DEBEN TENER EN CUENTA

El impacto en la empresa al no considerar como una prioridad la seguridad de la información, puede llegar a ocurrir que la información importante o confidencial de la empresa no este protegida y podría fácilmente ser robada o consultada sin autorización.

Dependiendo del tipo de información, el impacto puede ser determinado por la importancia de la misma [8], por su valor comercial, por su importancia de producto y marca, estratégica en el mercado, si son sus clientes y/o proveedores, sencillamente es el secreto de la empresa, el cual le da ventaja con respecto a sus competidores.

Es fundamental medir la eficiencia de las acciones implementadas para garantizar verdaderas mejoras y una gestión que no se quede sólo en el papel, el cambio de mentalidad en la organización es lo más complejo y lo que demandará más tiempo a los responsables de seguridad de información, ya que es un cambio cultural a todos los niveles y se evidenciara una resistencia al cambio en todos los niveles de la empresa "antes se hacían las cosas de x manera en esta empresa y funcionaba".

Es necesario que la alta gerencia tome conciencia de que la implementación de un SGSI es un factor vital para el éxito de la organización, lo apoye, se parte fundamental de todo el proceso de implementación, por otro lado encontrar personal con experiencia en temas de seguridad es bastante complicado y se debe también tener

Impulsar la creación de un Departamento de Seguridad la Información, es una necesidad, ya que es muy común que el área de I.T tenga labores de Seguridad Informática, sin diferencias procesos, y tener gente idónea para realizar estas labores.

X. ERRORES MÁS COMUNES

La implementación de un SGSI se está convirtiendo cada vez más en una obligación y porque no necesidad a nivel público y privado afectando a todo tipo de empresas, por esta razón se observa que el mercado laboral está en la necesidad de contar con mano de obra calificada para desarrollar, administrar y gestionar estos procesos.

Así mismo se observa que la cantidad de empresa que inicia su proceso de implementación de SGSI [10] es cada día más grande, detectando que se enfrentan en su día a día a muchos retos siendo los más

¿Una consultoría me resuelve el problema?

Posiblemente algunas empresas requieran tercerizar y acudir a consultorías externas para lograr sacar su proceso e implementación en el menor tiempo posible y con el menor margen de error y re procesos posibles, es decir dejarle el problema a un tercero para que se lo resuelva.

En cierta medida puede llegar a ser acertado buscar ayuda externa, pero siempre se debe tener en cuenta que la empresa consultora puede llegar hacer un buen análisis de riesgos siempre y cuando tenga toda la colaboración por parte del cliente para identificar los riesgos, analizarlos y valorarlos, seleccionar las opciones para su tratamiento, y para implantar el plan de tratamiento de riesgos con el que se pretende mitigar el nivel de riesgo detectado.

El éxito de la implementación del es directamente proporcional al trabajo en equipo con las partes interesadas y al nivel de madurez de la empresa en la gestión de la seguridad.

¿El área TIC es responsable de todo?

Como se trata de proteger la información crítica para el negocio, se deben ver involucradas todas y cada una de las áreas: Departamento TIC, RR.HH, Áreas: Financiera, legal, Marketing y todos aquellos que trabajan con esa información crítica para el negocio.

Todos deben ser sensibilizados de su responsabilidad en el SGSI.

¿A la deriva después de implementado?

Después de montado y puesta en marcha el SGSI es bastante común que las empresas queden desconcertadas y en proceso de transición con sus nuevos procesos y políticas andando a la deriva mientras todos en la empresa realizan su curva de aprendizaje, esta curva variara en el tiempo de acuerdo a varios factores, en este punto se sabrá si el SGSI fue bien diseñado desde el principio ya que como uno de los objetivos será el lograr que, cuando los procesos estén funcionando, se integren de la manera más transparente posible en el funcionamiento de la organización, y se vean afectados lo menor posible.

XI. CONCLUSIONES

Se debe construir un documento que describa las políticas y directrices a seguir, estas directrices deben ir orientadas a mantener un control eficiente y eficaz frente a la seguridad de la información.

Así mismo se debe tener conciencia de la importancia de involucrar a todas y cada uno de los empleados de la empresa y cada una de las áreas de la empresa, en todos los niveles, es importante en este punto tener identificadas las áreas y personas que van a estar fuera del SGSI, ya que por su actividad y función no requiera estar incluidas en el SGSI.

EL SGSI debe cumplir con las expectativas de la empresa así como con las proyecciones de negocio.

Las políticas y directrices no deben ser excesivas y que afecten el desarrollo del desempeño normal de la empresa.

Lograr un SGSI requiere que los procesos que conlleva se integren de manera lo más transparente posible en el funcionamiento de la organización y los procesos realizados.

REFERENCIAS

[1] © Copyright OSIATIS S.A. www.osiatis.es. Gestión de la Seguridad Introducción y Objetivos. [Online] Disponible: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_seguridad/introduccion_objetivos_gestion_de_la_seguridad/introduccion_objetivos_gestion_de_la_seguridad.php

[2] Acevedo Juárez, Héctor. (2011/11/08). ISO-27001: ¿Qué es y para qué sirve? (parte 1). [Online] Disponible: http://www.magazcitum.com.mx/?p=1574#.VlDiu3YvfIU

[3] Rodríguez, Adalberto Cervantes. (2014/09/25). La diferencia entre ITIL® y COBIT, en pocas palabras. [Online] Disponible: http://www.bitcompany.biz/diferencia-itil-y-cobit/#.Vl4zJnYvfIU

[4] ISO 27001: Desafíos para las organizaciones en Seguridad (2014/11/19). [Online] Disponible: http://www.pmg-ssi.com/2014/11/iso-27001-desafios-para-las-organizaciones-en-seguridad/

[5] MSC Zamora, Carlos Sotelo. (2012/10/09). Una perspectiva desde el Gobierno de TI. [Online] Disponible:http://seguridad2012.politicadigital.com.mx/pdf/12.pdf

[6] Acevedo Juárez, Héctor. (2011/11/08). Integrando Cobit, Itil e ISO 27000 como parte de Gobierno de TI. [Online] Disponible: http://www.magazcitum.com.mx/wp-content/uploads/2010/07/Integrando-CobiT-ITIL-e-ISO-27001-como-parte-del-Gobierno-de-TI.pdf

[7] Vargas, Ana Cecilia. Mattei, Alonso Castro. (2012/01/05). Sistemas de Gestión de Seguridad de la Información. [Online] Disponible: http://archivo.ucr.ac.cr/docum/ISOEIC27000.pdf

[8] Pacheco, Federico. (2010/09/10). La importancia de un SGSI. [Online] Disponible: http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

[9] Ramón Robles, Álvaro Rodríguez de Roa. (2010/06/01). La gestión de la seguridad en la empresa [Online] Disponible: http://www.aec.es/c/document_library/get_file?uuid=172ef055-858b-4a34-944d-8706db5cc95c&groupId=10128

[10] Vanaclocha, Patricia. (2010/03/29) Errores comunes en la Implantación de un SGSI. [Online] Disponible: http://www.securityartwork.es/2009/03/29/errores-comunes-en-la-implantacion-de-un-sgsi/